

The LDAP No-Op Control
<[draft-zeilenga-ldap-noop-03.txt](#)>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

This document is intended to be, after appropriate review and revision, submitted to the IESG for consideration as a Standard Track document. Distribution of this memo is unlimited. Technical discussion of this document will take place on the IETF LDAP Extensions mailing list <ldapext@ietf.org>. Please send editorial comments directly to the author <Kurt@OpenLDAP.org>.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts. Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as ``work in progress.''

The list of current Internet-Drafts can be accessed at <<http://www.ietf.org/ietf/1id-abstracts.txt>>. The list of Internet-Draft Shadow Directories can be accessed at <<http://www.ietf.org/shadow.html>>.

Copyright (C) The Internet Society (2003). All Rights Reserved.

Please see the Full Copyright section near the end of this document for more information.

Abstract

This document defines the Lightweight Directory Access Protocol (LDAP) No-Op control which can be used to disable the normal effect of an operation. The control can be used to discover how a server might react to a particular update request without updating the directory.

1. Overview

It is often desirable to be able to determine if a directory [[X.500](#)] operation would successful complete or not without having the normal effect of the operation take place. For example, an administrative client might want to verify that new user could update their entry (and not other entries) without the directory actually being updated. The mechanism could be used to build more sophisticated security auditing tools.

This document defines the Lightweight Directory Access Protocol (LDAP) [[RFC3377](#)] No-Op control. The presence of the No-Op control in an operation request message disables the normal effect upon the directory which operation would otherwise have. Instead of updating the directory and return the normal indication of success, the server does not update the directory and indicates so by returning the noOperation resultCode (introduced below).

For example, when the No-Op control is present in a LDAP modify operation [[RFC2251](#)], the server is do all processing necessary to perform the operation without actually updating the directory. If it detects an error during this processing, it returns a non-success (other than noOperation) resultCode as it normally would. Otherwise, it returns the noOperation. In either case, the directory is left unchanged.

This No-Op control is not intended to be to a "effective access" mechanism [[RFC2820](#), U12].

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [BCP 14](#) [[RFC2119](#)].

DN stands for Distinguished Name.

DSA stands for Directory System Agent.

DSE stands for DSA-specific entry.

2. No-Op Control

The No-Op control is an LDAP Control [[RFC2251](#)] whose controlType is IANA-ASSIGNED-OID, criticality is TRUE, and controlValue is absent. Criticality of TRUE is REQUIRED to prevent unintended modification of the directory. There is no corresponding response control.

The control is appropriate for LDAP Add, Delete, Modify and ModifyDN operations [[RFC2251](#)].

When the control is attached to an LDAP request, the server does all normal processing possible for the operation without modification of the directory. That is, when the control is attached to an LDAP request, the directory SHALL NOT be updated and the response SHALL NOT have a resultCode of success (0).

A result code other than noOperation (IANA-ASSIGNED-CODE) means that the server is not able or willing to complete the processing for the reason indicated by the result code. A result code of noOperation (TBD) indicates that the server discovered no reason why the operation would fail if submitted without the No-Op control.

Servers SHOULD indicate their support for this control by providing IANA-ASSIGNED-OID as a value of the 'supportedControl' attribute type in their root DSE entry. A server MAY choose to advertise this extension only when the client is authorized to use this operation.

[3.](#) Security Considerations

The No-Op control mechanism allows directory administrators and users to verify that access control and other administrative policy controls are properly configured. The mechanism may also lead to the development (and deployment) of more effective security auditing tools.

The No-Op control mechanism is believed not to introduce any security risks beyond those of the base operation it is attached to. Security considerations for the base operations, as well as general LDAP security considerations, are discussed in RFCs comprising the LDAP Technical Specification [[RFC3377](#)].

[4.](#) IANA Considerations

[4.1.](#) Object Identifier

It is requested that IANA assign an LDAP Object Identifier [[RFC3383](#)] to identify the LDAP No-Op Control defined in this document.

Subject: Request for LDAP Object Identifier Registration
Person & email address to contact for further information:
Kurt Zeilenga <kurt@OpenLDAP.org>
Specification: RFC XXXX
Author/Change Controller: IESG

Comments:

Identifies the LDAP No-Op Control

[4.2](#) LDAP Protocol Mechanism

Registration of this protocol mechanism is requested [[RFC3383](#)].

Subject: Request for LDAP Protocol Mechanism Registration

Object Identifier: IANA-ASSIGNED-OID

Description: No-Op Control

Person & email address to contact for further information:

Kurt Zeilenga <kurt@openldap.org>

Usage: Control

Specification: RFC XXXX

Author/Change Controller: IESG

Comments: none

[4.3](#) LDAP Result Code

Assignment of an LDAP Result Code called 'noOperation' is requested.

Subject: LDAP Result Code Registration

Person & email address to contact for further information:

Kurt Zeilenga <kurt@OpenLDAP.org>

Result Code Name: noOperation

Specification: RFC XXXX

Author/Change Controller: IESG

Comments: none

[5.](#) Author's Address

Kurt D. Zeilenga

OpenLDAP Foundation

<Kurt@OpenLDAP.org>

[6.](#) Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#) (also [RFC 2119](#)), March 1997.
- [RFC2251] Wahl, M., T. Howes and S. Kille, "Lightweight Directory Access Protocol (v3)", [RFC 2251](#), December 1997.
- [RFC3377] Hodges, J. and R. Morgan, "Lightweight Directory Access

Protocol (v3): Technical Specification", [RFC 3377](#),
September 2002.

7. Informative References

- [X.500] International Telecommunication Union -
Telecommunication Standardization Sector, "The Directory
-- Overview of concepts, models and services,"
X.500(1993) (also ISO/IEC 9594-1:1994).
- [RFC2820] Stokes, E., et. al., "Access Control Requirements for
LDAP", [RFC 2820](#), May 2000.
- [RFC3383] Zeilenga, K., "IANA Considerations for LDAP", [BCP 64](#)
(also [RFC 3383](#)), September 2002.

Intellectual Property Rights

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in [BCP-11](#). Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to

others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

